

Year-End Privacy Recap

January 7, 2020



Speakers



Doriann H. Cain

Partner
Faegre Drinker



Amy E. Keller

Partner
DiCello Levitt Gutzler



Jeremiah Posedel

Partner
Faegre Drinker

EU-US Data Transfers

How did we get here? The three “S”s –

- **Snowden, Edward**

- In June 2013, Snowden leaked information to the press about US intelligence gathering programs and the monitoring of phone and internet activity around the globe.

- **Schrems, Maximillian**

- After the Snowden revelations, Schrems pursued complaints against Facebook, arguing that Facebook had participated in the various intelligence gathering operations disclosed by Snowden in violation of EU law.

- **Safe Harbor, 2000-2015**

- Facebook defended its actions by reference to its Safe Harbor certification. This led to *Schrems I*, where the European Court of Justice determined that the bi-lateral Safe Harbor accord, negotiated between the US and EU, was invalid.

The Long Road to Schrems II

- **After Safe Harbor was invalidated, US and EU negotiators began work on a replacement agreement.**
 - Ultimately, **Privacy Shield** was adopted in July 2016.
- **In the meantime, the focus of the business and privacy advocacy community shifted to standard contractual clauses (SCCs)**
 - Adopted in 2001, 2004, and 2010, these terms can be added to a contract to permit data transfers outside the EU between the contracting parties.
 - Schrems challenged Facebook's use of SCCs beginning in 2015.
 - Facebook argued that its use of the clauses was appropriate, and – in the alternative – that its subsequent certification to the Privacy Shield permitted its data transfers.
 - In 2019, the case was argued at the CJEU.

Schrems 2, Privacy Shield 0

- **On essentially the same grounds used to invalidate the Safe Harbor framework five years ago, the CJEU determined that the Privacy Shield Framework was also invalid.**
 - CJEU found the scope of US intelligence gathering activities to go beyond that which was necessary and created disproportionate invasions of privacy.
 - CJEU also focused on a lack of formal protection for individuals under US law:
 - US intelligence gathering laws don't generally allow individuals to contest the government's activities
 - No US independent government authority responsible for monitoring intelligence agencies and protecting privacy rights
 - Non-binding policy statements made by US Government during Privacy Shield negotiations could patch over the absence of formal legal rights and oversight

Standard Contractual Clauses+

- Court found SCCs to be generally legally valid, but . . .
- Whether a particular arrangement was valid depended on whether the *importing* entity could fulfill its legal obligations under the SCCs.
- The CJEU explained that *both* parties had an obligation to evaluate the laws that apply to the data importer, and determine whether those laws “enable[] the recipient to comply with the standard data protection clauses”
- If the laws could prevent the importer from living up to its obligations, then the parties should either:
 - Adopt additional safeguards to address the gap, or
 - Not transfer the data.
- Many commentators and some DPAs have noted that, although the Court focused on the implications of Schrems II for transfers to the United States, the same arguments about government access to data could apply in a number of other countries outside the EU.

Does this apply to you? US National Security Laws 101

- **The Foreign Intelligence Surveillance Act (FISA) – Section 702.**

- Allows government authorities (usually the FBI) to obtain a secret court order (called a FISC) that compels an “**electronic communications service provider**” to provide “all information, facilities, or assistance necessary to accomplish the acquisition” of foreign intelligence information.



Like a secret warrant

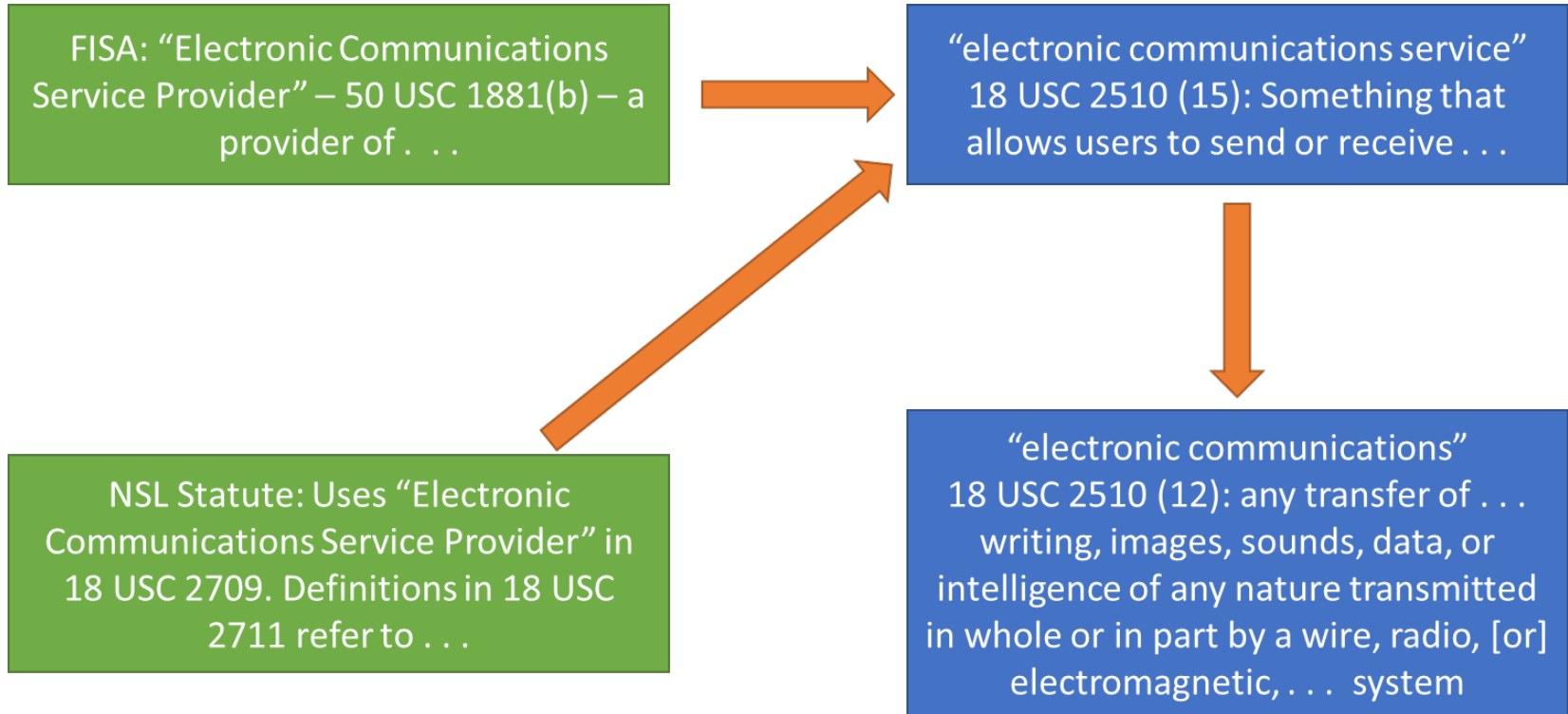
- **National Security Letters**

- Four statutes authorize law enforcement agencies to issue National Security Letters (NSLs) to obtain copies of certain business records (but not the content of communications).
- Statutes apply to financial institutions, consumer credit agencies, **electronic communications service providers**, and travel agencies.



Like a secret subpoena

Electronic Communications Service Provider – Many Statutes, One Definition

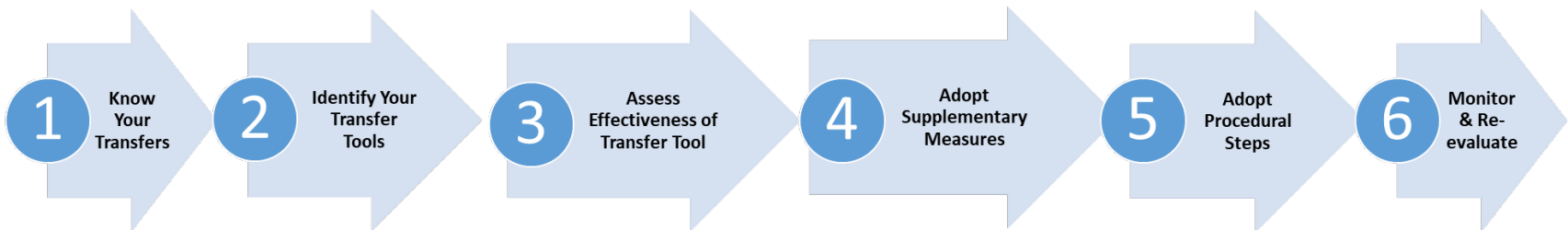


So . . . Wait. Who is an ECSP?

- **An electronic communications service provider can include not only traditional telecommunications companies but also anyone who:**
 - facilitates the transmission of electronic communications
 - or the storage and retrieval of electronic communications.
- **Examples:**
 - Providing email and phone services to a company's own employees
 - Online platforms that allow communications between users
 - Social media websites
 - . . . And more.
- **Because the *same definition* is used in statutes related to civil liability for ECSPs, this definition has been subject to much litigation in the US.**

EDPB's Recommendations

- **On 10 November, the EDPB published two guidance papers regarding cross-border data transfers:**
 - *Recommendations 01/2020 on Measures that Supplement Transfer Tools to Ensure Compliance With the EU Level of Protection of Personal Data*
 - *Recommendations 02/2020 on the European Essential Guarantees for Surveillance Measures*
- **6-Step Process**



Step 1 – Know Your Transfers

- **What Does this mean Practically?**
 - **Map** all transfers of personal data to third countries AND **verify** that the data you transfer is adequate, relevant, and limited to what is necessary in relation to the purposes for which it is transferred to and processed in a third-country.
 - EDPB highlights that controllers must take into account onward transfers and scenarios in which their processors in a third country may use sub-processors in another third-country or the same third-country.
 - EDPB notes that remote access from a third country and/or storage in a cloud situated outside of the EEA is also considered to be a transfer.

Step 2 – Identify Data Transfer Mechanisms

If you rely on an adequacy decision or Art. 49 derogation, you do not need to take any further steps.

- **Valid transfer mechanisms:**

- Adequacy decisions of the European Commission (see list [here](#));
- Derogations for specific situations under Art. 49 GDPR (e.g., prior consent of the data subject).

- Standard Contractual Clauses (SCCs) approved by the European Commission (Art. 46(2)(c) and (d) GDPR);
- Binding Corporate Rules (BCRs) approved by the European data protection authorities (Art. 46(2)(b), Art. 47 GDPR);
- "Ad-Hoc Clauses" approved by the European data protection authorities (Art. 46(3)(a) GDPR); and

- **After identifying the data transfers, you must verify the transfer mechanism that your transfer relies on.**

If you rely on an Art. 46 transfer tool, proceed to step 3.

Step 3 – Assess if Transfer Tool is Effective in Light of All Circumstances

- **Aka assess the law in the third country to which you are transferring data.**
 - Where organizations rely on Art. 46 transfer mechanisms, they must assess whether the non-EEA data importer is prevented from complying with its data transfer obligations due to legislation and practices applicable to the importer.
 - This step necessarily requires an assessment of the legislation applicable to the non-EEA data recipient, taking into account the nature, scope and circumstances of the transfer (e.g., amount and types of personal data subject to the transfer, and type of processing performed by the non-EEA data importer).
 - Specifically, the EDPB notes that controllers may “not rely on subjective [factors] such as the likelihood of public authorities’ access to your data in a manner not in line with EU standards” (Paragraph 42).
- **The EDPB recommends that data exporters request relevant information from the data importer to request relevant information applicable to it. The EDPB also suggests that data exporters request relevant information to research applicable legislation in the third country. See Annex 3 of the EDPB's [Recommendations](#).**

If your assessment reveals that applicable legislation affects the effectiveness of the transfer mechanism, data exporters should implement supplementary methods (step 4).

Step 4 – Adopt Supplementary Measures

- If the assessment in step 3 reveals that legislation applicable to data importers effects the effectiveness of the transfer mechanisms, data exporters should **implement supplementary measures in order to bring the level of protection of the data transferred up to EEA's standard of being essentially equivalent.**
- **Recommendations for supplementary measures:**
 - Technical Measures (e.g., encryption, pseudonymization, split-processing)
 - Contractual Measures
 - Organizational Measures

Step 5 – Adopt Necessary Procedural Steps

- **An organization must take any formal procedural steps the adoption of supplementary measures may require, depending on the specific Art. 46 transfer mechanism relied upon.**

SCCs

BCRs

Ad Hoc
Contracts

Step 6 – Re-evaluate at Appropriate Intervals

- **Organizations are responsible for monitoring developments in the third country to which they have transferred personal data that could affect your initial assessment of the level of protection.**
- **You should put in mechanisms to ensure you suspend or end transfers where:**
 - The importer has breached or is unable to honor the commitments it has taken in the Art. 46 transfer tool; or
 - The supplementary measures are no longer effective in that third country.

Use Case 2: Transfer of Pseudonymised Data

- ***A data exporter first pseudonymises data it holds, and then transfers it to a third country for analysis, e.g., for purposes of research.***
 - a data exporter transfers personal data processed in such a manner that the personal data can no longer be attributed to a specific data subject, nor be used to single out the data subject in a larger group, without the use of additional information,
 - that additional information is held exclusively by the data exporter and kept separately in a Member State or in a third country, territory or one or more specified sectors within a third country, or at an international organisation for which the Commission has established in accordance with Article 45 GDPR that an adequate level of protection is ensured,
 - disclosure or unauthorised use of that additional information is prevented by appropriate technical and organisational safeguards, it is ensured that the data exporter retains sole control of the algorithm or repository that enables re-identification using the additional information, and
 - the controller has established by means of a thorough analysis of the data in question taking into account any information that the public authorities of the recipient country may possess that the pseudonymised personal data cannot be attributed to an identified or identifiable natural person even if cross-referenced with such information,
- **the EDPB considers that the pseudonymisation performed provides an effective supplementary measure.**

IF...

THEN
...

Use Case 6: Transfer to Cloud Services Providers or Other Processors Which Require Access to Data in the Clear

- ***A data exporter uses a **cloud service provider** or other processor to have personal data processed according to its instructions in a third country.***

IF

...



- a controller transfers data to a cloud service provider or other processor,
- the cloud service provider or other processor needs access to the data in the clear in order to execute the task assigned, and
- the power granted to public authorities of the recipient country to access the transferred data goes beyond what is necessary and proportionate in a democratic society,

THEN

...

the EDPB believes that **NO** effective level of protection for data is possible.

Use Case 7: Remote Access to Data for Business Purposes

- “A data exporter makes personal data available to entities in a third country to be used for **shared business purposes**. A typical constellation may consist of a controller or processor established on the territory of a Member State transferring personal data to a controller or processor in a third country belonging to the same group of undertakings, or group of enterprises engaged in a joint economic activity.  The data importer may, for example, use the data it receives to provide personnel services for the data exporter for which it **needs human resources data**, or to **communicate with customers of the data exporter** who live in the European Union by phone or email.”
 - a data exporter transfers personal data to a data importer in a third country by making it available in a commonly used information system in a way that allows the importer direct access of data of its own choice, or by transferring it directly, individually or in bulk, through use of a communication service,
 - the importer uses the data in the clear for its own purposes,
 - the power granted to public authorities of the recipient country to access the transferred data goes beyond what is necessary and proportionate in a democratic society, **the EDPB believes that NO effective level of protection for data is possible.**

Where do we go from here?

- Accordingly, the EDPB appears to be saying that – in the scenarios described in Use Cases 6 and 7 – SCCs, BCRs, Codes of Conduct, Certifications, and an ad hoc contractual clauses may not be used and data may **only** be transferred to an adequate jurisdiction or pursuant to an Article 49 derogation.
- Given the above, what are our options?



Additional Contractual Measures

- **The EDPB notes that depending on what contractual measures are already included in the Article 46 GDPR transfer tool that is relied on, additional contractual measures may also be helpful to allow EEA-based data exporters to become aware of new developments affecting the protection of the data transferred to third countries.**
- **The recommendation provides examples of potential contractual measures regarding:**
 - Providing for the contractual obligation to use specific technical measures;
 - Transparency obligations;
 - Obligations to take specific actions;
 - Empowering data subjects to exercise their rights;
 - Internal policies for governance of transfers especially with groups of enterprises
 - Transparency and accountability measures
 - Organisation and data minimization measures
 - Adoption of standards and best practices

EDPB on European Essential Guarantees for Surveillance Measures

- **The EDPB's new recommendations update the original WP237 guidelines following CJEU's Schrems I judgment.**
- **The updated recommendations further develop the European Essential Guarantees in light of the Schrems II judgment.**
- **The specific Essential Guarantees analysed by the EDPB are:**
 - Guarantee A – Processing should be based on clear, precise and accessible rules;
 - Guarantee B – Necessity and proportionality with regard to the legitimate objectives pursued need to be demonstrated;
 - Guarantee C – Independent oversight mechanism; and
 - Guarantee D – Effective remedies need to be available to the individual.

The Commission Piles On...

- **On 11 November, the European Commission announced the beginning of a public consultation on its draft Implementing Decision on Standard Contractual Clauses for the Transfer of Personal Data to Third Countries and its Annex. The consultation period ended 10 December.**
- **The SCCs Draft Decision notes that the SCCs outlined in the Annex are considered to provide appropriate safeguards within the meaning of Article 46(1) and 2(c) of GDPR for the transfer of personal data from a controller or processor that is subject to the GDPR (data exporter) to a controller or (sub-) processor not subject to GDPR (data importer).**

CPRA

Overview

- **CPRA was a ballot measure created by Californians for Consumer Privacy, led by co-founders Celine Mactaggart and Alastair Mactaggart—chief architect of the California Consumer Privacy Act (CCPA)—to amend the CCPA and create new data privacy obligations.**
- **Ballot measure passed in November.**
- **Enters into force on January 1, 2023 and applies to personal information collected by businesses on or after January 1, 2022.**

Key Provisions

- **Service Providers**
 - Clarifies that “service providers” cannot combine personal information collected as a service provider with information received from other businesses or collected in the service provider’s “business” capacity (subject to exceptions).
- **Employee and Business-to-Business Exemptions**
 - Retains the CCPA’s exceptions for personal information collected in the employment and business-to-business contexts and extends their sunset provisions to January 1, 2023.
- **“Deidentified” Redefined**
 - Redefines “deidentified” to mean information that “cannot reasonably be used to infer information about, or otherwise be linked to, a particular consumer,” so long as the business takes reasonable measures to ensure that the information cannot be associated with a consumer or household, publicly commits to maintain information in deidentified form, and contractually requires recipients to comply with the provisions.

Key Provisions (II)

- **Pre-Collection Notice**

- Expands the information that a business must include in the pre-collection notice, including the categories of sensitive personal information collected and whether they are sold or shared; and the length of time the business intends to retain each category of personal information or the criteria that would be used to determine the retention period.

- **Storage Limitation**

- Prohibits retaining personal information for longer than is “reasonably necessary”.

- **Data Minimization**

- Limits collection, use, retention, and sharing of personal information to what is “reasonably necessary” to achieve the specified purposes.

- **Contracting Requirements**

- Requires businesses to enter into contracts with all entities to which the business discloses personal information.

Key Provisions (III)

- **Security Practices**

- Requires businesses to implement reasonable security procedures and practices appropriate to the nature of the personal information to protect the personal from unauthorized or illegal access, destruction, use, modification, or disclosure.

- **Deletion + Correction**

- Requires businesses to, in response to a valid deletion request, notify service providers and contractors to delete personal information and to notify all third parties to delete the personal information.
- Requires businesses to use commercially reasonable efforts to correct inaccurate personal information in response to a verifiable consumer request.

- **Right to Know**

- Expands the period of time covered by consumer right to know.
- Expands the scope of right to know requests to include a business' sharing and disclosure.

Key Provisions (IV)

- **Opt-Out of Sale and Sharing**

- Requires businesses to provide consumers with the ability to opt-out of sharing of personal information in addition to the existing right under the CCPA to opt-out of the sale of personal information.
 - *Sharing includes the transferring or making available personal information to a third party for cross-context behavioral advertising, regardless of whether consideration is exchanged.*
 - *Requires that opt-out links be updated to read “Do Not Sell or Share My Personal Information” link unless the business allows consumers to opt-out via an opt-out preference signal sent with the consumer’s consent via a mechanism conforming to specifications to be established by implementing regulations. If a business is providing the link, it can be combined with the “Limit My Use of Sensitive Personal Information” link discussed below, if applicable.*

- **Limit on Use and Disclosure of Sensitive Personal Information**

- Requires that businesses not use or disclose a consumer’s sensitive PI for purposes other than those necessary to provide the goods or services requested by consumers without providing consumers the right to limit the additional uses or disclosures.

Key Provisions (V)

- **Establishes the “California Privacy Protection Agency” to assume responsibilities for promulgating rules and enforcing the CCPA through administrative proceedings.**
- **Empowers the Attorney General (and eventually the California Privacy Protection Agency) to issue regulations on a wide range of topics.**
- **Eliminates the 30-day cure period following notice of alleged non-compliance.**
- **Adds a new penalty of \$7,500 for violations involving personal information of consumers whom the business knows to be under 16 years of age.**

State Data Security Legislation

State Breach Notification Statutes

- **Washington DC**

- Expanded definition of PI
- HIPAA exception
- Notification to AG – 50 or more DC residents
- 18 months credit monitoring

- **California**

- Expanded definition of PI

- **Maine**

- 30-day deadline for notification

- **Vermont**

- Expanded definition of PI
- HIPAA exception



NY SHIELD Act

- **Effective as of March 21, 2020**
- **Key components**
 - Expansion of Territorial Scope
 - Process PI of NY resident; even if no operations in NY
 - Expansion of the definition of “Private Information”
 - Expansion of the definition of a “Breach”
 - Imposition of “Data Security” Requirements
- **Compliance with other security laws (HIPAA, GLBA, NYDFS) constitutes compliance with SHIELD Act**
- **NY AG may bring a civil action that carries penalties up to \$5,000 per violation**
 - May bring action *before* a breach occurs, based solely on a company’s failure to implement reasonable data security safeguards
 - No private right of action

NAIC Data Security Statutes

- **Latest laws outgrowths of NAIC Insurance Data Security Laws**
- **Indiana**
 - NPI excludes business related information
 - Broader standard for authorized individuals
- **Louisiana**
 - NPI excludes business related information
 - Notification within 3 business days
- **Virginia**
 - Requires notification within 3 business days
 - Broad cybersecurity requirements but no multi-factor authentication
- **11 states have adopted the NAIC Data Security Model Law**

Emerging Trends

Cybersecurity Trends for 2021

- **Remote workers remain focus of cybercriminals**
 - Majority of companies have BYOD policies
 - Lack cybersecurity safeguards
 - Longer to identify and contain
- **Rise in cyber insurance**
 - Imperative to mitigate financial risks
- **Ransomware skyrocketing**
- **Healthcare devices next target**
 - Increase in implanted devices and wearables = increase in points of entry
 - Health care information is valuable

Federal Privacy Legislation

- **Internet of Things Cybersecurity Improvement Act**
 - NIST will develop minimum security requirements for IoT devices used by federal government
 - NIST publish guidelines on reporting security vulnerabilities
 - Adoption of coordinated vulnerability disclosure policies
- **Federal Privacy Law?**
 - Possibility pursued due to Schrems II
 - State legislation – added complexity
 - 2020 bills show narrow differences
 - Biden administration familiar with privacy legislation

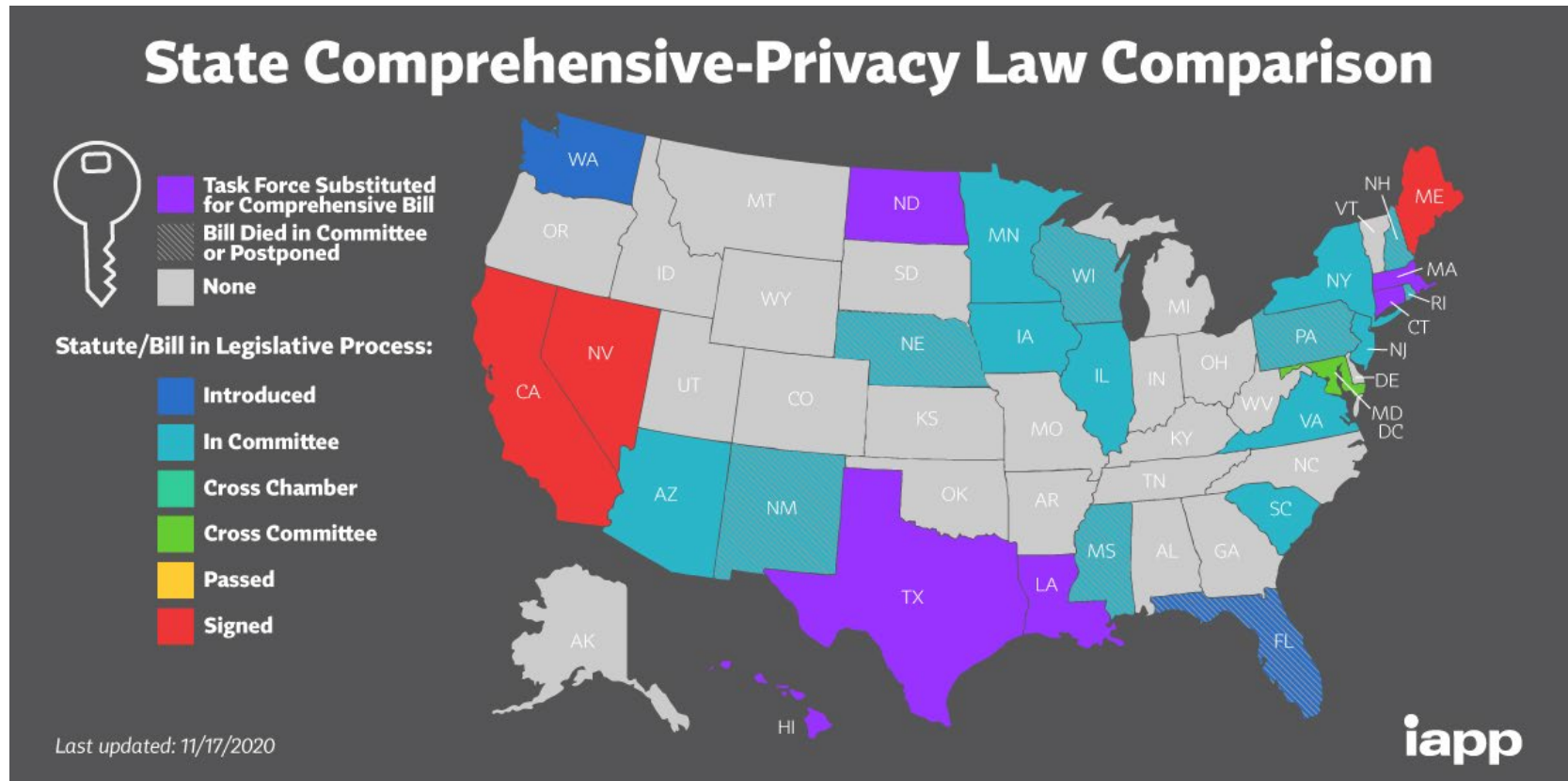
State Privacy Legislation

- **Washington Privacy Act**
 - Re-introduced for a third time
 - Touches on handling of data during public health emergency
 - Private right of Action BUT narrowed
 - Individual rights similar to CCPA and GDPR
 - WPA and CCPA contain varying definitions of “sale”
 - Legislative session begins January 11, 2021

Big Question...

- **What's the best way to address compliance?**
 - Jurisdictions?
 - Applicable laws?
 - Data?
 - Data flows/transfers?
 - Processing activities?
 - Risk tolerance?

State Privacy Legislation



<https://iapp.org/resources/article/state-comparison-table/>

Interface Webinar Series powered by Faegre Drinker

- **Sign up to receive an invite for the Interface Series by emailing Mesha Hegna Goodwill. (mesha.hegna@faegredrinker.com)**

Interface is a monthly webinar series hosted by Faegre Drinker's privacy, cybersecurity and data strategy (PCDS) team. Speakers include a who's who of the industry, from Faegre Drinker attorneys to technology, operations and regulatory experts.

Thank You

